Using Chebyshev Polynomial and Quadratic Bezier Curve for Secure Information Exchange

Dr. Hala Bahjet Abdul Wahab
Computer Science Department, University of Technology/Baghdad.
Email:Hala_bahjat@yahoo.com
Tanya AbdulSattar Jaber
Computer Science Department, University of Technology/Baghdad.
Email:tanyoshka2@yahoo.com

Received on:9/8/2015 & Accepted on:19/5/2016

ABSTRACT
Information exchange approaches are still an important research issue in the network security, generation and sharing the secret session key is the important factor during the group key transfer protocols. In this paper, we propose a new approach for information exchange based on PGP protocol as behavior. The proposed approach aims to combine chaotic techniques and curve security features based on chebyshev polynomial and quadratic Bezier curve, respectively to improve NTRU algorithm to increase the security features in the session key transfer process and improve DES algorithm in the encryption process. The proposed approach adds more security levels In the case of confidentiality and authentication with acceptable results.
Keyword: PGP, Chaotic system, Chebyshev polynomial, Curve security, Quadratic Bezier curve, Curve fitting.

INTRODUCTION
Secure information exchange covers different aspects to be considered, many of companies around the world facing similar problems and challenges when they try to share secret or sensitive information among users [1]. Chaotic maps are simple unstable dynamic systems this system has a high sensitivity to initial condition any small change in the initial condition lead to a large change in the corresponding orbits [2]. Curve security is frequently used in computers graphics and can add to cryptography to add more security to the system [3].Waale Mahdi Al bidire, (2014), produced system for generating a secure key from fingerprint based on the shape and the features of the ridge of the fingerprint by using cubic Bezier curve titled " **Fingerprint security approach for information exchange on network"**. The system describes three main stages (preprocessing of fingerprint, encryption and decryption with authentication stages). The authentication is a matching of the features of fingerprint. The equation of cubic Bezier curve converts thinning fingerprint to a matrix of control points. Where each segment of ridge visualizes by cubic Bezier curve to four points that store in a matrix. The receiver side redrawing the thinning fingerprint image from the control points matrix by Bezier equation and then matching for authentication and generate the same key that uses to decrypt the data file [5]. In this paper we will produce a new protocol for exchange secret information based on PGP protocol behavior, combine with new security techniques using chaotic system technique (Chebyshev polynomial) and curve security (Quadratic Bezier curve).

Theoretical Background
Chaotic system
A chaotic system has sensitive dependence on initial condition likeness to random behavior and continues broad band power spectrum [7]. Cryptography based on chaos theory has been studied

https://doi.org/10.30684/etj.34.5B.5
2412-0758/University of Technology-Iraq, Baghdad, Iraq

extensively because chaos features characterized as a best properties of diffusion and confusion which is very important properties for cryptography [8]. There have been a large amount of researches describe how to use chaotic system to design cryptography algorithm, and mostly describe the symmetric-key schemes [9].

Extendedchebyshev polynomial

Chebyshev polynomial is one of great importance in mathematic especially in approximation theory many researches have been written about this polynomial. Chebyshev polynomials which define on [-1,1] are very well understood but which have complex argument is less understood [10]. The extended chebyshev polynomial is chebyshev polynomial defined on finite field [11].

-Let T (N): {0, 1; N-1} → {0, 1; N-1}

The extended chebyshev$T_n(x)$ is defined as:

$T_0(x) = 1 \bmod N;$

$T_1(x) = x \bmod N; T_k(x) = 2x\ T_{n-1}(x) - Tn\text{-}2(x) \bmod N$ … (1)

Where :

x€ {0,1,2….N-1}| **N**: is large prime but some research said that **N** not should be large prime or result from two large prime , but for more security **N** is preferred to be large prime and **N+1** have a large prime factor when the equation is define over **GF(N)**[11].

Quadratic Bezier curve

Quadratic Bezier curve is described by three points, the first and last points represent the "anchors" of curve and the second one control the shape of the curve, the generated curve generate the first and last points and approximate the second one [12].

-Quadratic Bezier curve development:-Three control points p_0, p_1, p_2 and parameter t which it ranges between (0, 1).

- P_1^1 be a point on $\overline{p_0\ p_1}$ defined by:

$P_1^1 = (1-t)\ p_0 + t\ p_1$ …. (2)

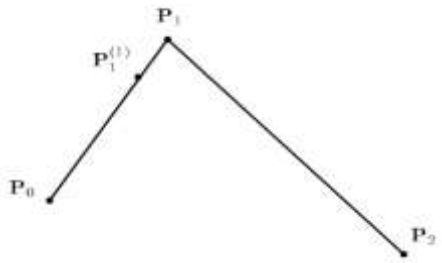

Figure (1): representation of P_1^1 point.

- P_2^1 be a point on $p_1\ p_2$ defined by:

$P_2^1 = (1-t)p_1 + t\ p_2$ …. (3)

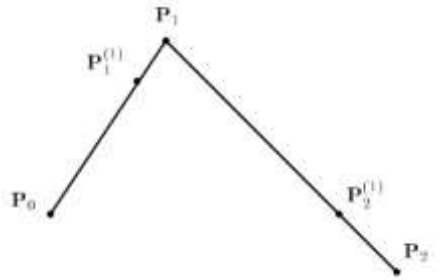

Figure (2): representation of P_2^1 point.

- P_2^2 be a point on p_1^1 p_2^1 defined by :

$$\mathbf{P_2^2 = (1-t)\, p_1^1 + t\, p_2^1} \qquad \text{..... (4)}$$

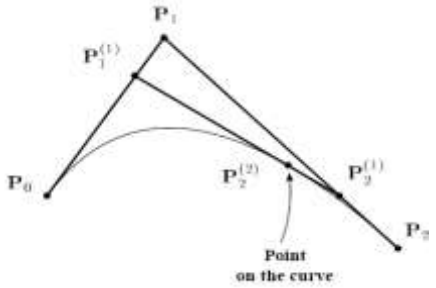

Figure (3): representation of P_2^2 point on curve.

- $\mathbf{P(t) = p_2^2 = (1-t)^2\, p_0 + 2t\,(1-t)\, p_1 + t^2\, p_2}$ ..... (5)
- Quadratic polynomial [13].

- $\mathbf{x(t) = (1-t)^2\, x_1 + 2t(1-t)\, x_2 + t^2 x_3,}$ …(6)
- $\mathbf{y(t) = (1-t)^2\, y_1 + 2t(1-t)\, y_2 + t^2\, y_3,}$ ……(7)
- $\mathbf{0 \le t \le 1}$, where (x, y) are the control points [13].

The proposed approach description

In this section the proposed approach is illustrated with describe the main approach stages, a new protocol for sending and receiving security information proposed. The protocol aim to increase the security level by adding a new hybrid approach the combine between chaotic techniques (extended chebyshev polynomial) and curve security concepts (quadratic Bezier curve) to the main stages of the proposed protocol (master key generation, encryption key generation, authentication) to increase the complexity, randomness and security features to the proposed protocol. The main stages of the proposed protocol shown in the figure (4):

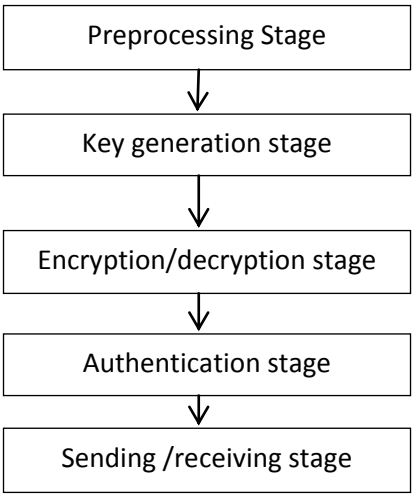

Figure (4): Block diagram for the main stage for the proposed approach.

Preprocessing stage

This stage applies on the plaintext to prepare it before the encryption stage. This stage compresses the plaintext to decrease the disk space, increase transmission speed and increase the processing speed.

Key generation stage

This stage describe the generation of all the encryption keys that proposed in this protocol, master key and session key, master key is the main key that generates the session key, session key is the key that use in encryption the plaintext.

Master key generation process

The main role of the master key in this approach is to generate the session key, this approach proposes a new method to generate the master key by using extended chebyshev polynomial equation (1), the result is a sequence of binary bits that represent the master key. Note that the sequence of the aster key could change in every session by changing the value of X in equation.

- ***Session key generation process*** This section offer a new method to generate the session key based on curve security concepts using quadratic Bezier curve equation, the master key will convert to set of control points to use it in quadratic Bezier equations (6) (7) and fitting the curve on random binary image, the result is a sequence of binary bits that represent the session key.

Encryption stage(as sending process)

The encryption stage in this approach includes two parts:

- **Encrypt the secure information process**The algorithm whichused in encrypt the plaintext in this approach is the traditional data encryption standard (DES) algorithm but after consuming the key schedule process and use instead the generated session key, after divide it into 16 blocks each one has 48 bits, this alteration will make the encryption process faster than regular DES process.
- **Encrypt the master key process**

In this approach the generated master key should send the cipher text to the receiver side, for that reason this approach should encrypt the master key with a public key algorithm before sending it, we used the improve NTRU algorithm that explain in [14] for encrypt this approach master key and send it as cipher key with the cipher text.

Authentication stage The authentication code or signature added to confirm to the receiver side that the message sent from known sender and didn't change in the middle way by any intruder or attacker, in this approach the Authentication code is a sequence of binary bits added to the end of the cipher text, this new approach propose a new method to generate the Authentication code by using quadratic Bezier curve equation and fitting the curve on plaintext image, the result is a sequence of binary bits that represent the authentication code, the deduction process done by a pre-agreed control points by the two sides sender and receiver also the structural of the deduction, in this method each time the plaintext change the deducted pixel of the authentication code will change too, so that any alteration in message by any intruder will discover by the receiver.

Decryption stage (as receiving process)

The decryption operation is apply in the receiver side when receive the cipher message, the first thing to do is take the last 64 bits of the cipher text that represent the authentication code and separated from the cipher text, then decrypt the master key that send with cipher message by using improve NTRU algorithm that explain in [14], after decrypt the key the receiver will convert the master key to set of control points and repeat the same steps to generate the encryption key by using quadratic Bezier curve equation and the same image that use by the sender, after generated the same key the receiver should divides the key into 16 blocks with 48 bits for each and reverse the key from last block to first block and enter to the DES algorithm todecrypt the cipher text, the result is the plaintext, to verify that the message is a same as origin and don't change by any intruder the receiver will convert the plaintext to image and apply the agreed method of deduction of the authentication code from the plaintext image by the same control points and the same equation of quadratic Bezier curve then compare it to the receive one if they similar then there is no alteration, if they different then the message change by an attacker.

- **In the following the main algorithmthat describe the proposed approach**

Algorithm:Sending process

Input: plain text, parameter value for chebyshev equation.
Output: cipher text, cipher key.
Process:
Step1: convert plaintext to binary bits.
Step2: generate master key by extended chebyshev polynomial and convert it to set of control points.
Step3: generate encryption key from the master key control points by using quadratic Bezier curve.
Step4: encrypt the plaintext with DES algorithm by using the generated encryption key.
Step5: generating authentication code by using quadratic Bezier curve equation fitting on plaintext image and added it to the end of cipher text bits.
Step6: encrypt the master key with improve NTRU algorithm [14].
Step7: send the block message of the cipher text and cipher key.
Step8: End.
In the following figures summarized the sending and receiving process based on the proposed approach.

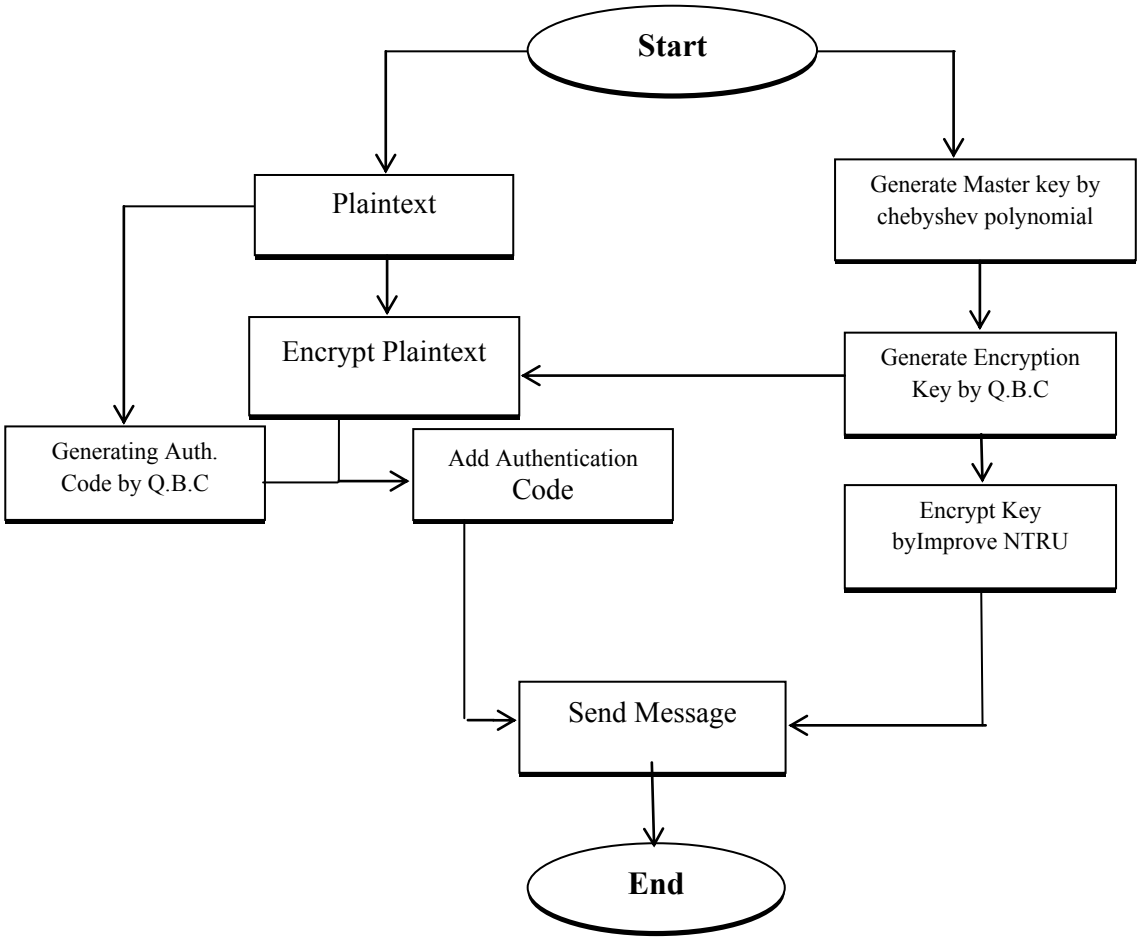

Figure (5):- Sender side.

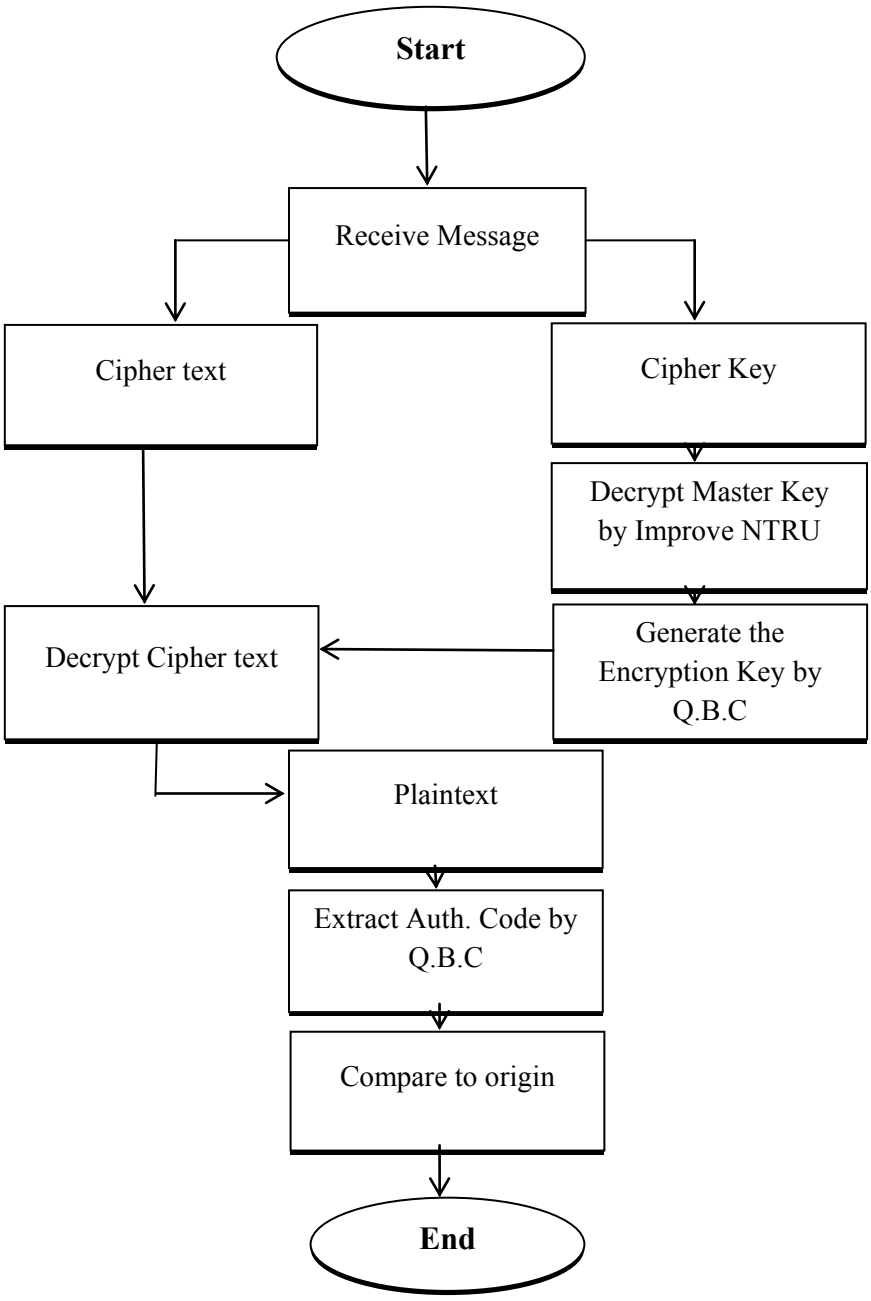

Figure (6):- Receiver side.

Experimental results

This section explained the implementation of the proposed approach for sending and receiving sides.

Key generation stage: generate master key from extended chebyshev polynomial equation and the encryption key from it, let N=13, x=2.

$T_k(x) = 2x\ T_{n-1}(x) - Tn\text{-}2(x) \bmod N$ …. (1)

$T_1(x) = x;$

$T_0(2)=1$, $T_1(2)=2$, $T_2(2)= (2*2*2-1) \bmod 13 =7$, $T_3(2)=(2*2*7-2) \bmod 13=0;$

The set of result is {1 2 7 0 6 11 12 11 6 0 7 2 1}.
The binary set {1000010011100000011011010011110101100000111001001000}.
The master key {1000010011100}.
Now convert the master key to control points by change each two bits to integer number, 10=2, 00=0, 01=1, 00=0, 11=3, 10=2,
We take the first number and the last to make the first point (2,2), and the second number and the fifth number to make the second point (0,3), and the middle numbers to make the third point (1,0), then substitute these points in quadratic Bezier curve equation

$$x(t) = (1-t)^2 x_1 + 2t(1-t) x_2 + t^2 x_3 \quad \ldots(6)$$
$$y(t) = (1-t)^2 y_1 + 2t(1-t) y_2 + t^2 y_3 \quad \ldots(7)$$

The resulting number of these equations fitting on binary image to take numbers of pixel that enough to make 16 keys with 48 bits for each, these bits will represent the encryption key.
Note: we take two bits binary in convert the integer number because N=13 we can take more than two bits if N bigger.

Encryption stage: encrypt the plaintext with the system encryption key.
The plaintext = security,
binaryplaintext=110011101010011011000110101011100100111010010110001011101001111 0 . Then
enter the plaintext to the DES algorithm with the 16 blocks keys to cipher the text.

Authentication stage: generate authentication code from quadratic Bezier curve equation fitting on plaintext image, let N=64, control points p1 (15,12), p2(19,20), p3(18,11).

$$x(t) = (1-t)^2 x_1 + 2t(1-t) x_2 + t^2 x, \quad \ldots\ldots(6)$$
$$y(t) = (1-t)^2 y_1 + 2t(1-t) y_2 + t^2 y_3 \quad \ldots\ldots(7)$$

the result of these equations fitting on plaintext image and deduct a series of binary bits these binary bits represent the authentication code for the message and add to the end of cipher text.
Authentication Code:
{000000000001111111111111111111111111111111111111111111111111111}.

Encrypt the master key process: encrypt the master key with improve NTRU algorithm,
master key = 1000010011100, N=13, q=32, p=3, pubic key H= (30 9 9 29 14 9 2 17 16 22 17 30 20), r= (-1 0 -1 0 0 -1 0 1 0 0 1 0 1),
Cipher session key = 29 21 30 2 0 13 2 28 15 26 16 21 26,
Now will send the message which consists of cipher text and cipher master key to the receiver which begin the decryption operation by reverse the above steps.

Decryption stage: decrypt the master key by the same algorithm improve NTRU algorithm, and generate the same encryption key.
N=13, q=32, p=3, f = (1 0 0 -1 1 -1 0 -1 1 0 0 0 1), g= (1 0 0 -1 -1 0 0 -1 1 0 1 0 0), f_q = (26 1 13 24 20 11 31 29 10 12 8 12 28), f_p = (2 2 1 2 1 1 0 1 0 2 0 0 1), cipher master key= 29 21 30 2 0 13 2 28 15 26 16 21 26.
a= (-8 -6 -8 -1 5 4 0 12 2 12 -6 -4 3),
b= (1 0 1 -1 -1 1 0 0 -1 0 0 -1 0),
c= (1 0 0 0 0 1 0 0 1 1 1 0 0) = master key.
Now convert the master key to control points by the same way that used by the sender p1=(2,2), p2=(0,3), p3=(1,0). Substitute in quadratic Bezier curve equation

$$x(t) = (1-t)^2 x_1 + 2t(1-t) x_2 + t^2 x_3, \quad \ldots(6)$$
$$y(t) = (1-t)^2 y_1 + 2t(1-t) y_2 + t^2 y_3 \quad \ldots(7)$$

The result numbers of these equations fitting on binary image to take numbers of pixel that enough to make 16 keys with 48 bits for each, these bits will represent the encryption key, This time the keys use by reverse from the last to the first.

Decryption stage: decrypt the cipher text with the generated encryption key. The generated 16 blocks of keys will enter the DES algorithm and decrypt the cipher text after separate the authentication code from the cipher plaintext= security, the receiving authentication code= {000000000001111111111111111111111111111111111111111111111111111111}.

Authentication stage: Extract the authentication code from the received plaintext image by quadratic Bezier curve, let N=64, control points p1 (15,12), p2 (19,20), p3 (18,11).

1- Convert the plaintext to image

2- Use quadratic Bezier curve equations (6) (7) to calculate the point that fitting on the plaintext image and extract the code.

3- Compare the extracted code with the received code.

Extractcode={000000000001111111111111111111111111111111111111111111111111111111}.

Receivedcode={000000000001111111111111111111111111111111111111111111111111111111}.

Performance

This section shows the performance of the proposed approach by measure the time that taken at main operation of the proposeNTRUImprovementbased on N number, and the time of encryption and decryption in improve DES algorithm.

Table (1): show the time of the main operation of improved NTRU on N=107

Main operation	Standard NTRU	Improved NTRU
Get r	15 ms	0.43 ms
Get g	14 ms	0.02 ms
Key generation	37 ms	36 ms
Encryption	36 ms	36 ms
Decryption	86 ms	65 ms

Table (2): show the time of encryption and decryption of improved DES

Main operation	Standard DES	Improved DES
Encryption	5 sec	7 ms
Decryption	8 ms	6 ms

Random tests

This section will show the measurements of randomness to each key that generated in the approach to prove the randomness and the security of each one.

Table (3): show the random tests measurements.

Tests	Master Key 107 bits	Improved DES Block Key48 bits	Traditional DES Block Key48 bits
Frequency	Pass 1.345	Pass 0.020	Pass 0.020
Serial	Pass 0.600	Pass 1.637	Pass 0.575
Run	Pass 4.056	Pass 2.333	Pass 4
Poker	Pass 1.923	Pass 0.5	Pass 3.38
Auto Correlation	Pass	Pass	Pass

CONCLUSION

The proposed approach succeed to represent anew secure information protocol based on improve NTRU algorithm. Using the robust security feature from chaotic techniques in NTUR algorithm increase the security feature with consuming time in improve NTRU algorithm according to the performance results (Table1). The proposed approach proposed new modification on key generation stage in DES algorithm and reduce the time operation by replacing the traditional key generation process in DES algorithm by new generation randomness keys based on curve security techniques with good results according to the randomness tests results(Table 3). The proposed approach succeeds to produce a new security protocol based on PGP behavior nature with fixable capability to improvement with consuming time.

REFERENCES

[1].Tobias Christen, Patrick Greuter, Anton Heer, Lukas Ruf, Martin Sibler, Walter Sprenger, Rudolf Studer, Erich Vogt, "Secure Information eXchange" Whitepaper of the SGRP Special Interest Group "Secure Information eXchange (SIX)" in collaboration with ISSS, 2011.

[2].George Makris ,Ioannis Antoniou, "Cryptography with Chaos" ,Proceedings, 5th Chaotic Modeling and Simulation InternationalConference, 12 – 15 June 2012, Athens Greece

[3].Dr. HalaBahjat Abdul wahab, Dr. RanaFareedGhani. "Quantum Description of Curve Cryptography Technique to Implement Key Distribution System".Department of Computer Science University of Technology, Journal of information technology, 2008.

[4].Hilal M. Yousif Al-Bayatti1,Abdul Monem S. Rahma2 and HalaBahjat Abdul Wahab, "PGP Protocol and Its Applications" from Book Cryptography and Security in Computing,Applied Science University, Kingdom of Bahrain Computer Science Depart , University of Technology, Baghdad, Iraq,InTech,(2012).

[5].Waale Mahdi Al bidire, Wesam Sameer bahea,"fingerprint security approach for information exchange on network", European Journal of Scientific Research, Vol.123, No. 2, pp: 169-181 (2014).

[6].Maryam Ahmed, BaharanSanjabi, DifoAldiaz, AmirhosseinRezaei, HabeebOmotunde, "Diffie-Hellman and Its Application in Security Protocols",International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012

[7].LjupcoKocareva and MarjanSterjevb,Institute for Nonlinear Science, University of California,AttilaFeketec and Gabor Vattayd,Department of Physics of Complex Systems of the EotvosLorand University, "Public-key encryption with chaos", American Institute of Physics, 2004.

[8].Wang Xing-Yuan and Luan Da-Peng , "A secure key agreement protocol based on chaotic maps", Chinese Physical Society and IOP Publishing Ltd, 2013.

[9].Jinhui Sun, Geng Zhao, Xufei Li, "An Improved Public Key Encryption Algorithm Based on ChebyshevPolynomials",TELKOMNIKA, Vol. 11, No. 2, February (2013).

[10].Seon-Hong Kim, "Some properties of Chebyshev polynomials", Kim Journal of Inequalities and Applications, Korea, 2012.

[11].JyothsnaIvaturi, K.Ravindra, Y.Ramesh Kumar, "A Secured Multicasting Key and Data Exchange By Using Extended Chebhysev Map", International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014.

[12].Jim Armstrong, "Quadratic Bezier curve", TecNote TN-05-003, 2005.

[13].Kenneth I. Joy, "QUADRATIC BE´ ZIER CURVES". Visualization and Graphics Research Group Department of Computer Science University of California, Davis, (2000).

[14].Asst.Prof. Dr. HalaBahjet Abdul Wahab ,TanyaAbdulsattarJaber , "Improve NTRU Algorithm Based On Chebyshev Polynomial", Computer Science Department, University of Technology, The World Congress on Information Technology and Computer Applications 2015 WCITCA'2015 2015.